Kongeriget Danmark

Patent application No.: PA 2002 00387

Date of filing: 13 March 2002

Applicant: (Name and address)
SDC af 1993 Holding A/S
Borupvang 1
2750 Ballerup
Denmark

Title: Method of and system for processing transactions
IPC: G07F 19/00; G07F 7/00

The attached documents are exact copies of the filed application

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Patent- og Varemærkestyrelsen
Økonomi- og Erhvervsministeriet

07 March 2003

Pia Høybye-Olsen

PATENT- OG VAREMÆRKESTYRELSEN

Method and system for processing transactions

The present invention relates generally to processing of transactions to and/or from mobile stations (e.g. mobile telephones i.e. cellular phones).

More particularly the invention relates to:

- A method of issuing a mobile cheque according to claim 1. A preferred embodiment is described in detail in paragraph 5.3 especially 5.3.2;
- A method of making a deposit of a mobile cheque via SMS according to claim 4. A preferred embodiment is described in detail in paragraph 5.4 especially 5.4.2;
- A method of making a withdrawal of cash according to claim 8. A preferred embodiment is described in detail in paragraph 5.5 especially 5.5.2; and
- A method of making a withdrawal of cash from a cheque/deposit cheque via an Automatic Teller Machine (ATM) according to claim 11. A preferred embodiment is described in detail in paragraph 5.6 especially 5.6.2.

Other aspects of the invention relates to a registration procedure (see paragraph 5.1) and an activation procedure (see paragraph 5.2).

The present invention will be described in the following in accordance with preferred embodiments.

1.1 Terminology

This section defines the terminology used in the document:

Authentication Code	The first 8 bytes of a message digest calculated on, among other things, the public key and a One-Time-Password.
Mobile Equipment	The Mobile Equipment has all the functions for radio communication with the system. The ME together with the SIM equals the MS. Without the SIM it is only possible to do emergency calls.
Mobile Phone	Equivalent to the term Mobile Station as defined in GSM.
Mobile Station	In GSM used to define the phone. Divided in the two logical units Mobile Equipment and Subscriber Identity Module.
PIN-RSA	Specific PIN for access to private RSA key.
Short Message Entity	An entity capable of receiving and/or sending short messages. The SME may be located in for example the MS or in the fixed network.
Subscriber Identity Module	The SIM-card is a smart card that is used for storing of subscription-related information. The ME together with the SIM equals the MS.

1.2 Abbreviations

AT	ATtention
ATM	Automatic Teller Machine
BFC	BookKeepingCentral, BKC
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile communications
GW	Gateway
ISDN	Integrated Services Digital Network
MAC	Message Authentication Code
ME	Mobile Equipment
MS	Mobile Station
MSISDN	Mobile Station ISDN
OTA	Over The Air
OTP	One-Time-Password
PIN	Personal Identification Number
PIN-RSA	Personal Identification Number-RSA
PKCS	Public Key Cryptography Standards
RSA	Rivest, Shamir, Adleman
SDC	Sparekassernes DataCenter
SIM	Subscriber Identity Module
SM	Short Message
SME	Short Message Entity
SMPP	Short Message Peer to Peer protocol
SMS	Short Message Service
STK	SIM Application Toolkit

1. RSA Laboratories "PKCS #1 v2.0: RSA Cryptography Standard", October 1998, http://www.rsa.com/rsalabs/pkcs/
2. Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS); Point-To-Point (PP) (GSM 03.40)

2 Functional Overview

The SDC Mobile ATM Service makes it possible to withdraw cash from an ATM equipped with an IR-device (pay-box) over an infrared connection using an IR-enabled mobile phone and a specific SIM application.

When the user wants to withdraw cash, the user starts the ATM application via the service menu on the phone and enters the amount and the account that the money should be withdrawn from. Next, the user signs the withdrawal transaction and steps up to an ATM and points the infrared eye of the mobile phone towards the infrared eye of the pay-box. The pay-box sends a transaction request to the mobile phone where it is displayed and the user is requested to accept the transaction. The signed transaction is returned to the pay-box for further delivery to the bank. The bank performs the necessary authentication of the user and, if successful, transfers the money between the user's account and ATM where the user receives the cash.

The SDC Mobile ATM Service also introduces the concept of mobile cheques, which allows a user to issue a mobile payment to another user. The receiver of the mobile cheque will then be able to withdraw the issued amount of cash (or parts of it) from an ATM or deposit the amount to one of the bank accounts that the receiver possesses via SMS.

The security in the service is based on digital signatures, which are calculated by the SIM application when the user confirms a transaction in the mobile phone. The signature and relevant parameters are then sent via either IR or SMS to the bank where the signature is verified and the transaction is carried out. The SDC Mobile ATM Service concept will be an alternative to using credit cards in an ATM and a service for mobile payments between users.

2.1 Involved Entities

In the initial phase (pilot), the system is quite simple. It consists of several banks connected to one BFC, one operator and one SIM-card supplier. The idea is that the concept will support several operators, several SIM suppliers and several BFCs.

In later stages the system might become more complex, as depicted below:

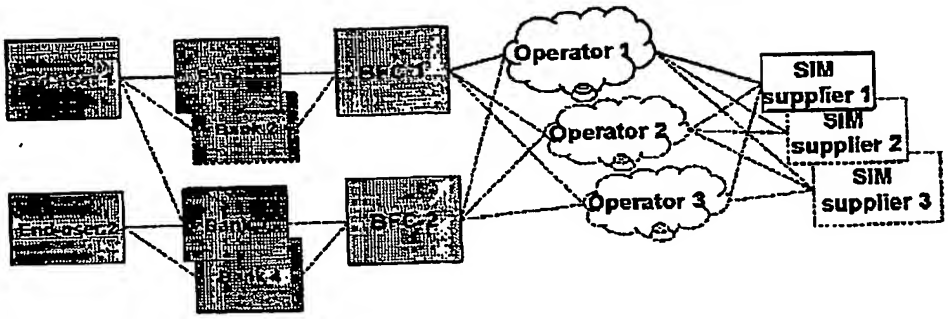

Figure 1: Involved entities

2.2 Over-The-Air Data Download Overview

On the user's side there is a need to store application data related to the ATM Service. This information must be configured for the service to work and must be possible to update to reflect changes made by both the customer and the bank. The information update is handled by Over-The-Air (OTA) updates using mobile terminated and mobile originated short message services. The requests are pushed from the bank domain, via an operator's GSM environment, to the user's mobile phone. In the mobile phone an application receives the information, verifies that it is correct and received from the correct source and stores it in file(s) on the SIM card.

The need for OTA updates of application data on the SIM card is related to two areas:

- Application configuration during activation of the service.

  During the activation procedure, the BFC provides the SIM application with the necessary bank and customer related application information.

- Service Management purposes

  When the service has been activated and is in use, it should be possible to change the status of the service (block/unblock) as well as the status on a specific account (block/unblock).

A request for an OTA update can be initiated in different situations and by different parties as given below:

- By the BFC/Bank at reception of an activation request (mobile originated short message) from the user. The BFC/Bank responds to the activation request by returning application data.

- By the user upon request, through the Internet Bank, to block or unblock the service.

- By the Bank upon request from bank system management personnel through the bank terminal, to block or unblock the service. This must have been originally initiated by the user for example by calling customer care (helpdesk).

- By the Bank upon request from bank system management personnel through the bank terminal, to block or unblock an account.

Both user and bank personnel can initiate OTA update requests. The user initiates these requests when logged on to the Internet bank, and since the Internet bank is hosted in the BFC domain no further authentication is needed.

The requests initiated by the bank are probably issued from a remote terminal in the bank, which is on a secure connection, and where administrative personnel must be authenticated before access is allowed.

It is the responsibility of the Bank application at the BFC to make sure that the entity (e.g. user, bank1, bank2...) requesting an operation has the permission to do it. The bank gateway will assume that appropriate access control has been performed by the Bank application prior to sending the request onwards.

3 Service System Architecture

This section is an overview of the system architecture, from the user's point of view, within the SDC Mobile ATM Service. The system architecture consists of the domains, nodes and roles outlined in the figure below.

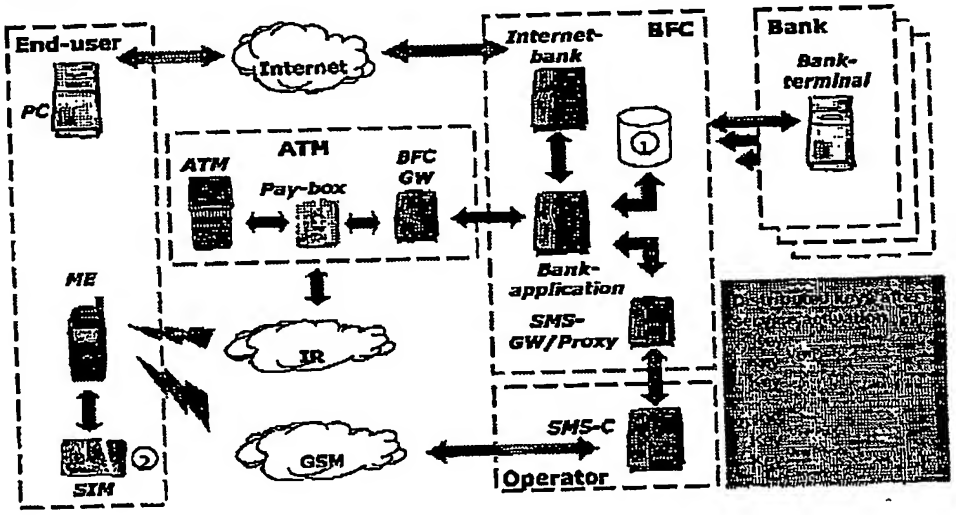

Figure 2: SDC Mobile ATM Service system overview

3.1 Information Exchange between BFC and Mobile Phone

The OTA updates are performed by sending application specific messages from the Bank application to the mobile phone via the BFC's SMS Gateway/Proxy and the operator's SMS-C. The application messages are transferred as user data within short messages and are transported between the mobile phone and the SMS-C using mobile originated and mobile terminated short messages. The protocol data units that are used to transfer the data are fully defined in chapter 7 in Ref **[Fejl Henvisningskilde ikke fundet.]**.

3.2 End-user Domain

After registration through the Internet Bank the user receives a new SIM card from the operator where the user is a subscriber. This SIM card contains the Mobile ATM Service STK application and it is personalised to allow remote updates OTA. However, the activation procedure must be successfully executed before it is possible to use the service.

Once the service is activated, the user uses a GSM mobile phone with infrared communication capabilities together with the customised SIM. The application on the SIM card is responsible for signing mobile cheques and ATM transactions and for the interaction with the user.

The information exchange between the mobile phone and the pay-box of the ATM is based on sending AT commands over the infrared connection. The information exchange between the issuer and the receiver of a mobile cheque is carried out over SMS with assistance from a SMS proxy server in the BFC domain.

3.3 ATM Domain

The following entities are part of the ATM domain:

- Pay-box

  The ATM is equipped with a pay-box supporting infrared communication capabilities and AT commands for communication with the mobile phone.

  The pay-box is responsible for fetching the transaction request and signed transaction from the mobile phone. The signed transaction fetched from the mobile phone is forwarded to the back-end financial system through the BFC gateway. It is assumed that the pay-box is connected to the BFC GW via a local network.

  The pay-box also communicates with the ATM, for example at initiation and completion of the money transfer procedure.

- ATM

  The ATM is responsible for the cash withdrawal and money transfer operations initiated by the user. The ATM receives the transaction request from the user via the pay-box and supplies the pay-box with additional parameters to be signed by the user.

  When the transaction is authorised and completed by the bank the ATM is asked by the pay-box to dispense the cash.

  Note: During a transaction with a mobile phone the keypad of the ATM is not used, all interactions by the user are via the mobile phone.

- BFC Gateway

  The BFC GW is responsible for forwarding the cash withdrawal and cheque deposit transactions performed by a user at an ATM. The transactions are forwarded to the bank domain over the banks private network, to the WEB server within the BFC domain.

3.4 BFC and Bank Domain

The BFC domain may consist of several Bank domains, i.e. several banks that are linked to the ATM Service and are using the same BFC for processing of the transactions.

The BFC domain can be divided into one BFC and several bank areas. The BFC is responsible for hosting some of the functionality that might be common between banks e.g. the Internet bank(s).

3.4.1 SMS Gateway/Proxy Interface

The BFC domain has an interface to the operator's GSM environment. The bank's SMS gateway is responsible for communication with the SMS-C within the operator domain.

The Bank application within the BFC domain communicates with the SMS Gateway/Proxy using an XML interface. With this interface it is possible for the BFC to request OTA updates of application information on the SIM card. The XML interface includes the receiver's phone number and a string to be sent either as an ordinary text message or an application message destined for the SIM application. The XML documents are sent between the Bank application and the SMS Gateway/Proxy using the HTTP method POST. The XML interface is further described in chapter 5 in Ref [2].

The SMS Gateway/Proxy also has a service listening for mobile originated messages. This service handle all messages from the mobile phone (independent of whether it's a mobile originating request or a response of a mobile terminated request) and delivers the messages as a XML document to the bank domain.

For information transferred in the direction Bank application to SMS Gateway/Proxy, the Bank application acts as HTTP client and the SMS Gateway/Proxy acts as HTTP server. In the opposite direction, SMS Gateway/Proxy to Bank application, the reverse applies, i.e. the SMS Gateway/Proxy acts as HTTP client whereas the Bank application acts as HTTP server.

3.4.2 Gateway functionality

The mobile terminated short messages destined for the SIM application must be coded as SMS Point-To-Point Data Download messages. This enables the ME to transparently forward the short messages to the SIM. To achieve this the short message parameters Data Coding Scheme and Protocol Identifier must have the following values (see Ref. [2] and Ref. **[Fejl! Henvisningskilde ikke fundet.]**):

- Data Coding Scheme: 0xF6 or 0x16

  The value of the parameter Data Coding Scheme must indicate 8 bit data and Message Class 2 (SIM specific message)

- Protocol Identifier: 0x7F

  The value of the parameter Protocol Identifier must indicate SIM Data download

The mobile terminated short messages containing an ordinary textual message intended to be displayed to the end-user on the mobile phone must not use the values defined above. In this case the short message parameter Data Coding Scheme and Protocol Identifier should have the following values.

- Data Coding Scheme: 0x00

  The value of the parameter Data Coding Scheme must indicate Default alphabet (i.e. the textual message is coded with 7-bit alphabet in packed format).

- Protocol Identifier: 0x00

  The value of the parameter Protocol Identifier indicates mobile phone to SMS-C message transfer.

3.4.3 Proxy functionality

In the Mobile ATM Service the SMS Gateway must also function as a proxy. The proxy functionality is needed to be able to send a message, coded as a SMS Point-To-Point Data Download message, from one mobile phone to another.

The requirements on the proxy are as follows:

- Must check all mobile originating messages and depending on the MessageType set, route the message to either the bank domain or forward the message to another mobile phone.

  On messages sent from one phone and forwarded to another (mobile cheques), the proxy should perform the following:

  - Take the Receivers phone number (MSISDN_receiver) from the mobile originating application message and put it in the SM header as the Destination Address.
  - Take the Originating Address from the mobile originating SM header and put it in the application message as a parameter for the sender's (issuer's) phone number (MSISDN_issuer).
  - Append the actual date from the proxy server to the application message as a parameter (ChequeIssueDate).
  - Code the mobile terminated message as SMS PP DD.

The short message flow between entities in the ATM Service can be summarised in the picture below:

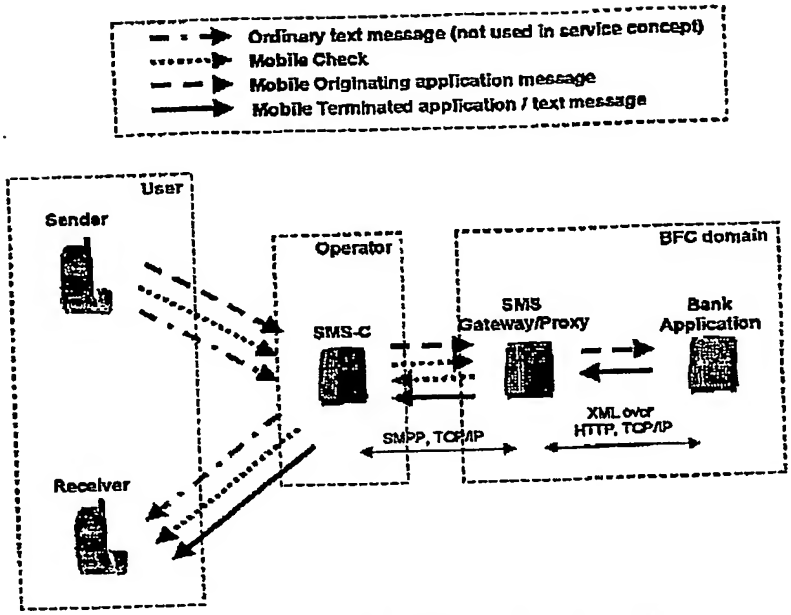

Figure 3: SDC Mobile ATM Service SMS overview

3.5 Operator Domain

The information in this chapter relates to the communication between the SMS Gateway/Proxy and the SMS-C and is transparent to the Bank application.

The SMS Gateway/Proxy within the BFC domain is connected to the operator's SMS-C using an SMS-C protocol, such as SMPP. The SMS-C is responsible for sending short messages to the mobile phone upon request from the SMS Gateway/Proxy as well as forwarding short messages originated from the mobile phone to the SMS Gateway/Proxy.

The mobile originated short messages are addressed to a specific SME address, a so-called large account. The SMS-C maps the SME address to an address to the SMS Gateway/Proxy and forwards the message to the SMS Gateway/Proxy within the BFC domain. The sender of the message, i.e. the MSISDN of the mobile phone, must be transferred from the SMS-C to the SMS Gateway/Proxy for further delivery to the Bank application.

4 Mobile Phone - SIM Interaction and SIM Aspects

The pay-box communicates with the mobile phone via AT commands over an IR connection. The mobile phone transforms the AT commands to ETSI 11.11 and 11.14 commands when communicating with the SIM. Hence, the actual AT command ends in the mobile phone, see picture below.

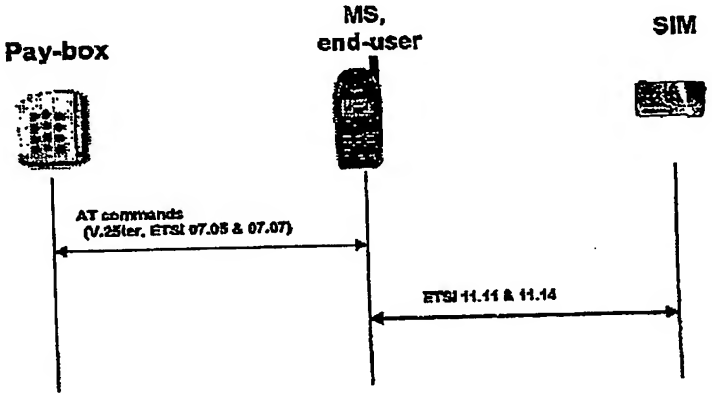

Figure 4: Standard interfaces used

The pay-box – mobile phone AT interface is fully described in Ref. **[Fejl! Henvisningskilde ikke fundet.]**. Basically the pay-box writes a request to the SM file and later reads the response from the SM file. The flow is schematically described below.

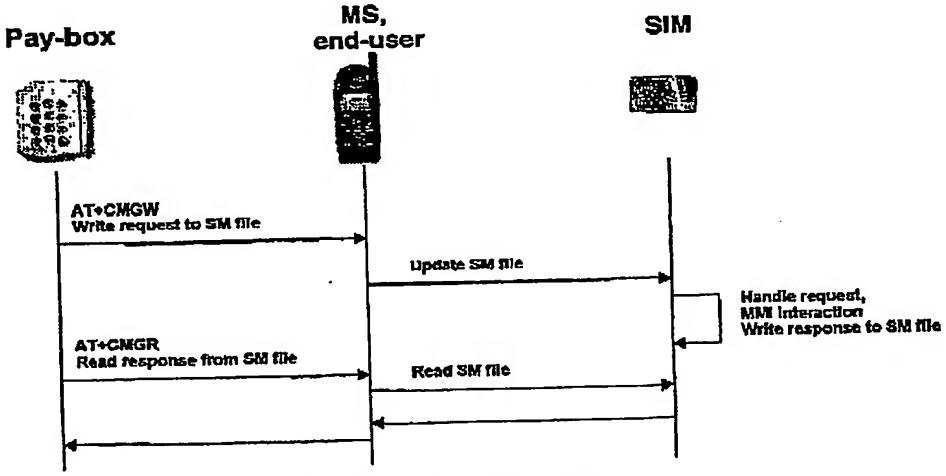

Figure 5: Using the SM file for requests and responses

The mobile phone is transparent in the pay-box – SIM communication. The ATM functionality is implemented as a separate SIM application

placed on the SIM card and called the Mobile ATM Service SIM application.

The ATM Service SIM application is triggered when a mobile cheque is received, when the user initiates an ATM or cheque transaction via the application menu and when an ATM transaction is received from the ATM's pay-box.

4.1 Mobile ATM Service SIM Application

The ATM SIM application provides the following functionality:

- Implementation of the MMI; i.e. user dialogue and error handling.
- Storage of various application parameters; e.g. UserID, BFCID, AccountId, AccountNickname etc.
- Generation and storage of the user's public and private key, storage of the BFC's public keys and the user's authentication code, PIN-RSA.
- Public key exchange.
- Handling of incoming requests from ATM, i.e. Profile, Transaction and Signature requests.
- Handling of cheque transactions, incoming cheques and deposit of cheques via SMS.
- Storage of received and issued mobile cheques.
- OTA support for configuration of application parameters.
- Blocking of service and accounts via OTA.

5 User Scenarios

This section describes the message sequence and steps performed in different user scenarios. The functionality performed by each node in the use cases is described as well as the interaction between the different nodes. It should be noted, though, that the interaction between pay-box and ATM, pay-box and BFC Gateway and the interbank communication is provided with less detail.

Note: The names and use of messages and parameters in this document are only for illustrative purposes and should not be interpreted as neither specification nor implementation details.

The different scenarios in the ATM service are listed here:

Activation

- Registration from Internet bank
- Activation from Internet bank to receive One-Time-Password
- Activation from mobile phone that performs public key exchange and application data download

Main functions

- Issue mobile cheque
- Deposit mobile cheque to account via SMS
- Withdraw cash from account via ATM
- Withdraw cash from mobile cheque (or deposit cheque) via ATM

Service management

- Block/unblock service, issued by user.
- Block/unblock account, issued by bank.
- Change PIN-RSA
- Setting of default account

5.1 Registration to the ATM Service

This section describes what happens when the user registers to the ATM Service. The sequence covers the interaction between the user and the Internet Bank.

Precondition: The user is a registered user of the Internet Bank and thus a trust relationship already exists between the user and the bank.

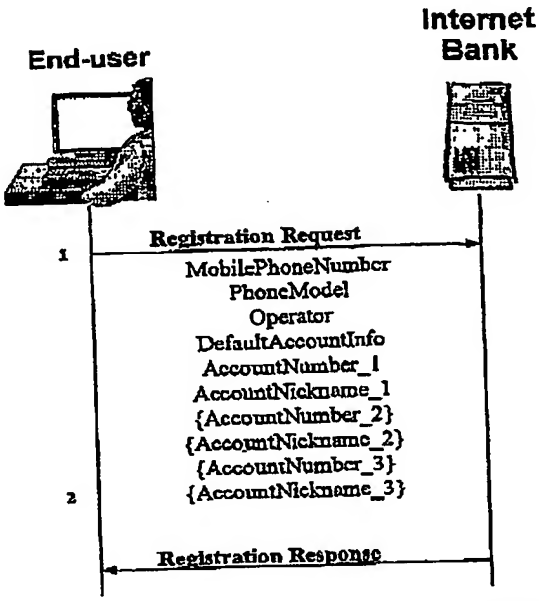

Figure 6: Message sequence flow during registration

The user selects a menu choice in the Internet Bank to register as user of the Mobile ATM Service and enters the required information. The following information must be defined upon registration:

- MobilePhoneNumber

  This is the GSM MSISDN of the mobile phone subscription.

- PhoneModel

  This information could be used by the Internet Bank to validate if the mobile phone is appropriate to use for the Mobile ATM Service e.g. that it has an IR device.

- Operator

  This is the GSM network operator where the user's is a subscriber.

- AccountNumber

  This is an account that the user has selected to use with the Mobile ATM Service and from which money will be withdrawn and deposited. In the pilot the user will be able to select at most 3 accounts.

- AccountNickname

  This is a user-defined nickname related to a specific Account Number. The nickname will be displayed to the user on the mobile phone when withdrawing cash from an ATM, issuing new cheques and cashing in cheques.

- DefaultAccountInfo

  This parameter is the identifier of the account the user has defined as default account. If default account is set, the account will be used in the transactions and the user will not be prompted to choose account. There will neither be any possibility to step backwards in the transaction flow to change account.

After the user has registered to the service, the bank will send a request to the operator for issuing and distribution of a new SIM card supporting the ATM Service application.

5.2 Activation of ATM Service

This section describes what happens when the user receives the new SIM card and activates the ATM Service. The sequence covers the interaction between the user and the Internet Bank as well as the user and the BFC domain.

Precondition: The user has received a new SIM card from the operator and has been instructed to activate the service through the Internet Bank. The mobile phone is switched on and the new SIM card inserted.

5.2.1 Activation Through Internet Bank

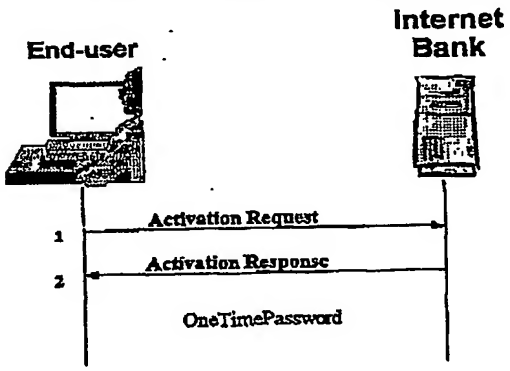

Figure 7: Message sequence flow during activation through Internet Bank

1. The user selects a menu choice in the Internet Bank for activation of the ATM Service.
2. An 8-digit One-Time-Password (OTP) is displayed to the user on the screen. This information is used in the SIM application to provide user authentication and initiate the key generation.

The user is instructed to select the menu choice for activation of the service on the mobile phone. (The sequence continues below in section 5.2.2.)

5.2.2 Public Key Exchange

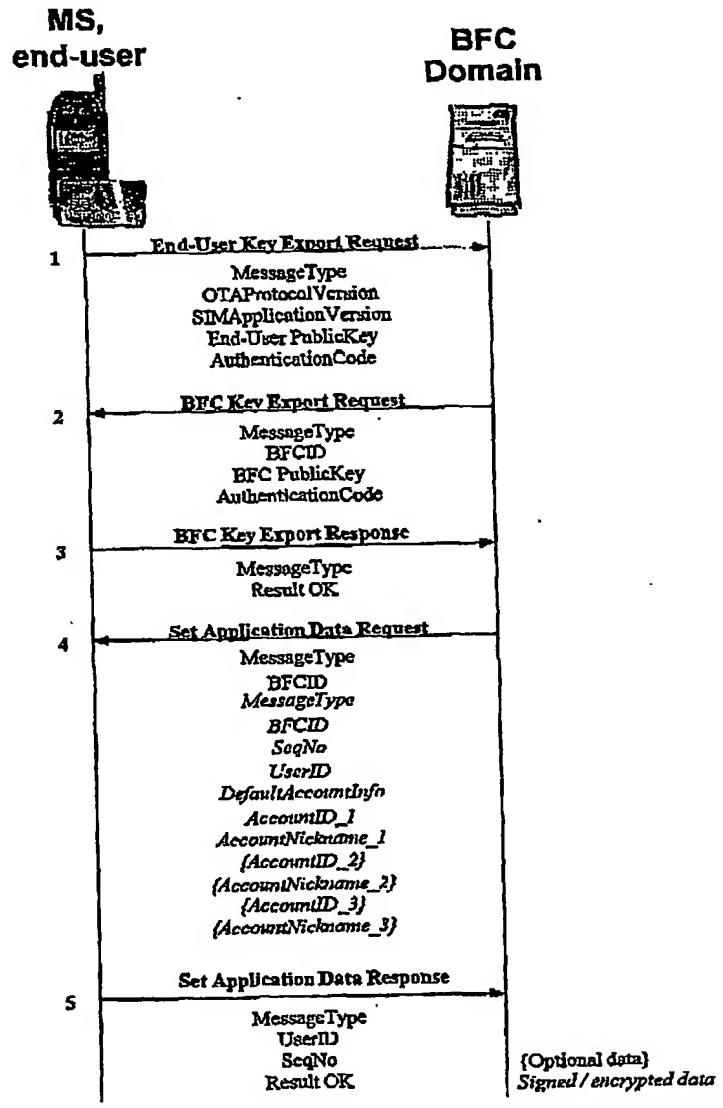

Figure 8: Message sequence flow during public key exchange. Note: The picture only show the parameters relevant for the ATM service.

1. The user selects the ATM Service activation in the menu on the mobile phone and enters the OTP.

Entering the OTP triggers generation of the RSA key pair on the SIM card. The private key is stored in a tamperproof location on the SIM card.

The application on the SIM card calculates an Authentication Code according to section 7.2.1. The input is all information in the message, i.e. the message type, the OTA protocol version, the SIM application version, and the public key of the user, concatenated with the OTP. The generated 8-byte Authentication Code is then sent together with the other parameters in a SM to the BFC domain.

Note: A SME address (phone number) is needed on the SIM card to send messages to the BFC domain. In the pilot the SME address is pre-configured on the SIM card, but this may not be feasible later on in a multiple BFC environment. The SME address may then be displayed to the user on the computer screen together with the OTP, and then entered into the mobile phone after the OTP.

2. Before the public key is accepted for use within the BFC domain, the Authentication Code received from the mobile phone is compared with an Authentication Code calculated locally in the BFC domain on the same parameters. If the comparison is successful the public key is stored.

   If the public key of the user is accepted the BFC domain exports its own public key, which will be used for server authentication purposes in subsequent operations.

   The message contains a new Authentication Code, which makes it possible for the application on the SIM card to verify that the message is originated from the correct source. It also contains the BFCID, which is used by the phone to link the public key to the correct BFC (in a multiple BFC scenario).

   The Authentication Code is calculated according to section 7.2.1. The input is all information in the message, i.e. the message type, the BFCID, and the public key of the BFC, concatenated with the OTP. The generated 8-byte Authentication Code is then sent together with the other parameters in a SM to the mobile phone.

3. When the message is received, the application on the SIM card validates the Authentication Code by comparing it with an Authentication Code calculated locally in the mobile phone on the same parameters. If the validation is successful, the public key is stored and the BFC domain is notified of the result.

4. The BFC domain then sends a message to the mobile phone containing the information required for configuration of the application on the SIM card. The information package is signed (encrypted) with the BFC's private key before it is sent to the mobile phone. This makes it possible for the SIM application to perform server authentication upon reception of the message.

In addition to the application information, the signed message contains the Message Type, the BFCID and a sequence number. The Message Type and the BFCID are also sent unencrypted, as the SIM application needs these parameters in order to handle the message. The signing of the message is performed according to section 7.2.3.

5. When the message is received, the SIM application verifies the signed message and checks the sequence number according to section 7.2.3. The BFCID is used to select which public key is used to verify the message.

   If the validation is successful, the application data is stored and the BFC domain is notified of the result. The sequence number received in the request from the BFC is returned in the response and could be used on the server side to link the result to the corresponding request.

   The user is requested to select a PIN code of 4 digits, which will be used to get access to the key files on the SIM card (referred to as PIN-RSA in this document). Finally, the user is informed that the service has been activated through a text message on the mobile phone display.

5.2.3 Error Cases, Activation

The following situations have been identified as error cases.

1. Key generation failure

   If the key generation on the SIM card fails, the user is prompted to try again by entering the OTP in the phone.

2. Key transfer failure, no response from the server

   If no response is received from the server after the public key has been exported, the user has to initiate the activation procedure again on the phone and enter the OTP. The previously generated public key will be exported and no new keys will be generated. The SIM application will not keep track of more than one key exchange request, i.e. only the last entered OTP will be kept and used to validate the Authentication Code of the response message. A second delayed response messages from the server will be discarded.

3. Key transfer failure, error message from the server

   If an error response is received from the server after the public key has been exported, the user can try to enter the OTP again. No new keys will be generated, but the Authentication Code will be calculated again using the new OTP input.

   If three error responses have been received from the server, the OTP will be used up and the user has to initiate the activation procedure again through the Internet Bank to retrieve a new OTP. The previously generated public key will be exported and no new keys will be generated.

4. Server does not receive an acknowledgement after successful activation

   The server must keep track of a timer and terminate the activation procedure after a certain period of time if an acknowledgement message has not been received. For security reasons the timeout should occur after a maximum of 30 minutes. However, if the activation has been completed in the phone (i.e. the PIN-RSA has been selected but the server has not received the acknowledgement message), the user can start to use the service.

5. User does not select a PIN-RSA when activation download is completed

   If the user does not select a PIN although the key transfer was successful, no acknowledge is sent back to the server. From the server perspective this is treated as the previous error situation and the activation procedure is terminated after a certain period of time. For security reasons the timeout should occur after a maximum of 30 minutes.

   Note: The timeout in the phone for entering the PIN-RSA will typically occur after a few minutes, but the server must take into account possible network delays of the acknowledgement message.

   Since the OTP has already been used during the key exchange, the user has to initiate the activation procedure again through the Internet Bank to retrieve a new OTP. The previously generated public key will be exported and no new keys will be generated.

6. User tries to activate the service again after successful activation.

   If the user selects the activation menu in the phone after successful activation of the service, a warning/information message will be displayed, but the user will be allowed to continue. The previously generated public key will be exported.

   Note: Only one bank will take part in the pilot, but later when several banks are involved, the user must activate the service and export the public key to each bank he or she wants to use.

5.3 Issue mobile cheque

This section describes what happens when the user uses the service to issue a mobile cheque to another user. It covers the steps performed and message sequence between the mobile phones of the issuer and receiver of the cheque.

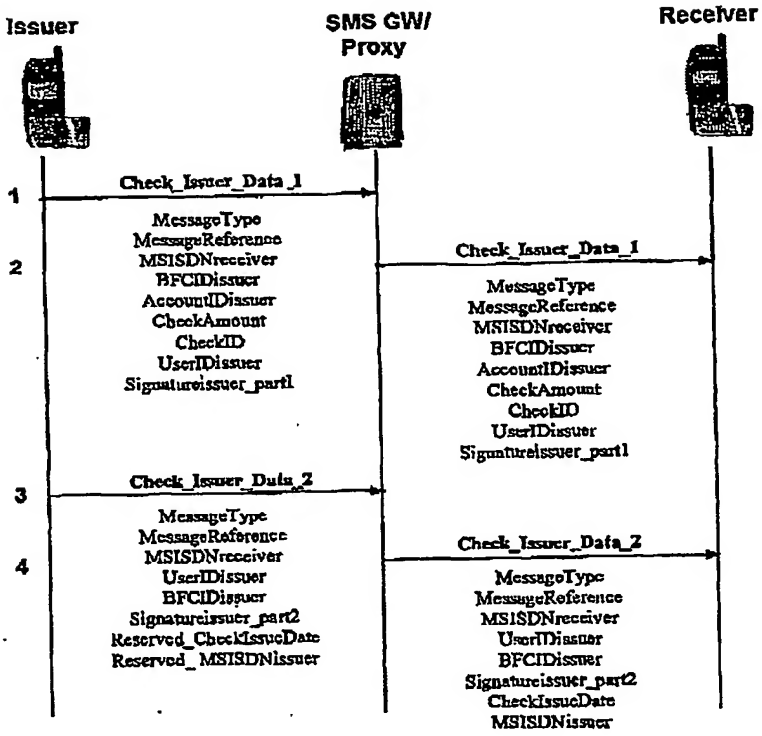

Figure 9: Message sequence during issuing of mobile cheque.

5.3.1 Preparation

When the user wants to issue a cheque the application is started via the appropriate menu entry in the service menu. The user is then prompted to enter the phone number of the receiver, the amount and, if no default account is set, the account that the cheque's amount should be withdrawn from. Finally the user is requested to enter the PIN-RSA code to be authenticated by the SIM application.

The phone number to the receiver must be entered as an international number as described in section 6.2 and the amount must be entered as described in section 6.1.1 to be accepted by the SIM application.

Before the cheque is sent a summary of the collected information is displayed to the user. The user confirms the Issue Cheque transaction by pressing Yes/Ok. In the summary a 3-digit cheque identifier is also displayed. For details on the signature and the data that it is based on, see section, 7.2.4.

Note: A cheque is valid for a limited time period set by the bank. A cheques' valid time is counted from the time the cheque is sent i.e. the date when it passes the issuer's bank's SMS Gateway/Proxy server.

5.3.2 Message sequence

A cheque is sent via SMS to the receiver via a SMS GW/Proxy in the issuer's BFC domain. No result or notification is sent back to the issuer.

1. When the cheque information is confirmed and signed by the issuer, the cheque is sent via SMS.

   Due to the large amount of information and the signature in a cheque, it has to be sent as two short messages. The signature is split into two parts and the cheque is then sent as two SM, with one part of the signature in each. To be able to associate the messages again on the receiver's side each message must contain a reference to the other part of the message; this parameter is called the MessageReference and is a one-byte counter that is unique for each user.

   Both messages must include the phone number (MSISDN) of the receiver to allow the SMS proxy to forward the messages to the receiver.

2. To be able to trig the application on the receiver side the SM has to be coded as a SMS PP DD message. The SMS proxy server is used to re-code the SM and to send it forward to the receiving mobile phone.

3. The second part of the cheque sent from the issuer to the receiver, containing the second part of the signature.

4. To be able to trig the application on the receiver side the SM has to be coded as a SMS PP DD message. The SMS proxy server is used to re-code the SM and to send it forward to the receiving mobile phone.

   Since an SMS Proxy is used, it is also be used to automatically append the MSISDN of the issuer. This is performed because the issuer of the cheque has to be presented to the receiver by a unique text string, in this case the phone number.

   Also added by the SMS Gateway/Proxy to the cheque is a date-stamp. The date stamp provides an issue date to the cheque and allows the bank to verify the validity time for the cheque. The date stamp is in the date format, YYYYMMDD.

5.3.3 Error Cases, Issue Cheque

The following situations have been identified as error cases.

1. Short message is lost

   If either of the 2 short messages, which make up a cheque, is lost the check cannot be saved by the receiver's SIM application. Neither issuer nor receiver will be notified if the receiver fails to receive a complete cheque (both messages making up the cheque). If the receiver did not receive the cheque, the issuer can send it again. To

send a cheque again the *Resend* command in the service menu should be used to make sure it is the same cheque that is sent again and not a new one being issued.

2. Issuing user enters wrong telephone number (unknown MSISDN)

   If the issuer has entered a phone number that is not valid, the SMS Gateway will receive the cheque via the issuer's operator's SMS-C and then forward the cheque via the same SMS-C. This will fail because the SMS-C is not able to forward the cheque to a "known" user.

3. The receiver of a cheque has not yet activated the service

   A user that has not activated the service will not be notified by an incoming cheque, neither will the cheque be stored.

4. The receiver of a cheque is "offline"

   If the receiving user has the mobile phone switched off when someone sends a cheque to that user, the short messages making up the cheque will be stored in the SMS-C for a certain time. This time is operator dependent but is usually a couple of days. If the user turns on the phone again within this time, the cheque will be received.

5. The receiver of a cheque is occupied in the service (SIM application busy)

   If the receiving user is busy using the SIM application for some task e.g. changing PIN code or preparing a purchase, when someone sends a cheque, the short messages making up the cheque can not be received by the SIM application. Instead the messages will be stored in the SMS-C for later delivery for a certain time period. This time is operator dependent but is usually a couple of days. When the user exits the application, the cheque will be received.

6. The receiver's Received Cheque file is full

   If the receiving user's cheque file is full (with complete un-deposited cheques) a message is displayed to the user saying that the cheque just received could not be saved. Note: The user was notified when a cheque was saved to the last empty position and instructed to free some cheque positions by depositing one or more cheques.

5.4 Deposit mobile cheque via SMS

This section describes what happens when the user uses the service to deposit a mobile cheque via SMS. It covers the steps performed and message sequence between the mobile phone of the receiver and the receiver's BFC.

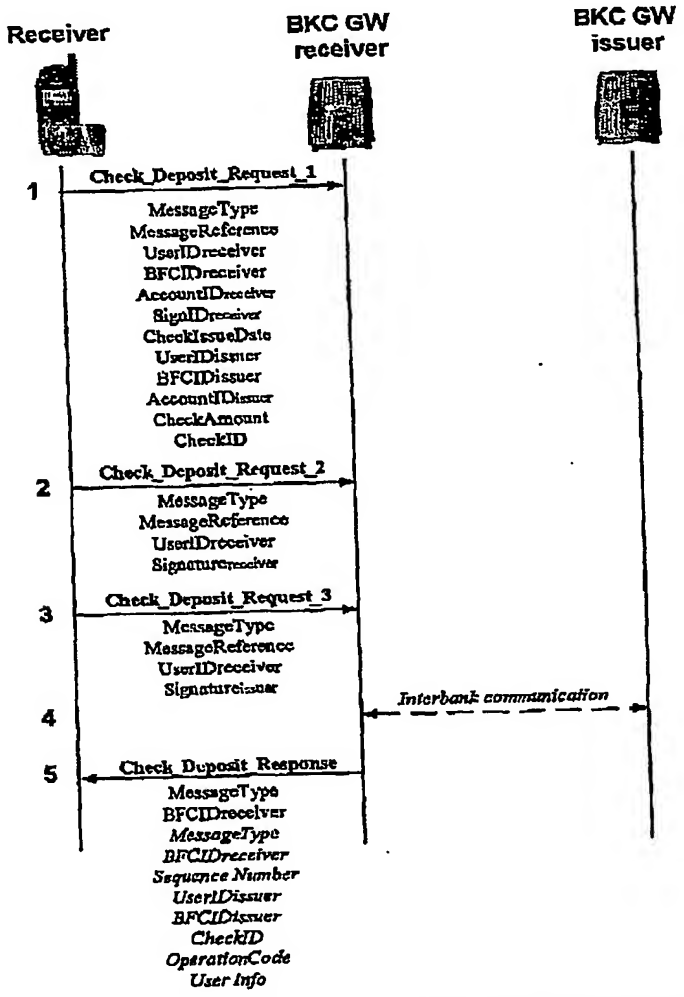

Figure 10: Message sequence during deposit of mobile cheque via SMS.

5.4.1 Preparation

When the user wants to deposit a received cheque to a bank account, it can be done both via SMS and as a special case via an ATM. The SMS case is described here.

The user enters the application via the appropriate menu entry in the service menu and is presented with a list of all received cheques. In the next interactions the user chooses the cheque that should be deposited and, if no default account is set, also chooses the account that it should be deposited to and enters the personal service PIN code to allow the transaction to be signed.

Before the request is sent a summary of the collected information is displayed to the user. The information displayed is amount, account nickname, date and a reference number. The reference number shown is a transaction identifier concatenated with the signature identifier. The transaction identifier is in this case set to a dummy value, "0000", since no transaction identifier is supplied by a pay-box. The user confirms the Deposit Cheque transaction by pressing Yes/Ok and the request is sent via SMS to the bank.

For details on the signature and the data that it is based on, see section, 7.2.4.

5.4.2 Message sequence

A deposit transaction is sent via SMS to the cheque's receiver's BFC gateway. A result message is sent from the receiver's bank domain to the receiver's mobile phone when the transaction has been completed between the two banks.

1. When the summary is confirmed and signed by the receiver of the cheque the deposit request is sent. Due to the large amount of information and the need to include both the issuer's and the receiver's signatures, the request has to be sent as three short messages. The first SM contains the cheque information and the next two short messages contain the signatures of the receiver and the issuer respectively.

   To be able to associate the messages again on the receiver's side each message must contain a reference to the other parts of the message; this parameter is called the MessageReference and is a one-byte counter that is unique for each user.

2. The signature of the receiver of the cheque is sent from receiver to the BFC GW of the receiver.

3. The signature of the issuer of the cheque is sent from receiver to the BFC GW of the receiver.

4. Communication between the receiver's bank and the issuer's bank.

   The receiver's bank verifies the receiver's signature and if successful sends the transaction to the cheque's issuer's bank.

   The issuer's bank verifies the issuer's signature and verifies that the receiver's MSISDN belongs to the user that the issuer intended. Additional verifications can be made. The bank verifies that the cheque

has not been deposited before by looking at the cheque Identifier. The bank verifies that the cheque is still valid by comparing the Cheque Issue Date on the cheque with the actual date and the validity time set according to the bank's policy. And the bank verifies that the issued amount on the cheque is available on the issuer's bank account.

If everything is successful the issuer's bank completes the money transfer to the receiver's account.

5. An application message is sent to the mobile phone from the receiver's bank to confirm that the deposit cheque request has been received. The message trigs the SIM application and displays a text informing the user of the result of transaction. The application message also contains an operation code informing the application to either remove the cheque or keep the cheque. Both the text and operation code is defined by the bank.

5.4.3 Error Cases, Deposit Cheque

The following situations have been identified as error cases.

1. Short message is lost

   If any of the 3 messages, which make up a Cheque Deposit request, is lost the bank can not interpret the incoming request. The bank should wait a certain time for further incoming parts of the request since a message can be delayed due to e.g. peak network traffic. If the complete request is not received within the specified the bank should send a response message, Cheque Deposit Response, to the user. This response should contain a suitable textual message to the user and instructions to the SIM application to handle cheque removal. In this case it is suitable not to remove the cheque, in order to allow the cheque receiver to deposit the cheque at a later time.

2. No cheque clearance on issuer's account

   A cheque can be issued from an account even if the account holds no money i.e. the clearance validation is not made until the cheque is deposited or withdrawn by the receiver. If the issuer's account lacks the issued cheque's amount at the time of deposit, the money transfer will fail. The Issuer's bank informs the unsuccessful result to the receiver's bank, which sends a Cheque Deposit Response to the receiver with the result of the operation. This response should contain a suitable textual message to the user and instructions to the SIM application to handle cheque removal. In this case it is suitable not to remove the cheque, in order to allow the cheque receiver to deposit the cheque at a later time.

3. Lost response message

   If, for some reason, the Cheque Deposit Response message never reaches the receiver's mobile phone e.g. the user might have turned off the mobile phone after the transaction, the user will not be informed of the result of the transaction. Neither will the SIM application receive

any instruction whether to remove the cheque or not. The result is that the cheque is "orphaned" and will not be deleted.

4. Invalid cheque (already used)

   A cheque that has been deposited via SMS should have been removed by the deposit operation's response message. If this is not the case, the user might try to deposit the cheque again and this will result in that the cheque identifier will be identified as already used in the issuer's bank. The issuer's bank notifies the receiver's bank, which sends a Cheque Deposit Response to the receiver with the result of the operation. This response should contain a suitable textual message to the user and instructions to the SIM application to handle cheque removal. In this case it is suitable to remove the cheque to avoid that the receiver tries to deposit the same cheque again.

5. Invalid cheque (validity time passed)

   The issuer's bank compares the Cheque Issue Date on the cheque with the actual date and the validity time set according to the bank's policy. If it is found that the validity time has passed the cheque is declared invalid and the user is informed with the Cheque Deposit Response. This response should contain a suitable textual message to the user and instructions to the SIM application to handle cheque removal. In this case it is suitable to remove the cheque since it will never be possible to deposit (or withdraw).

6. Receiver signature verification failure

   If the receiver's bank fails to verify the receiver's signature it is assumed that the user claiming to be the recipient is not or that the parameters has been corrupted during transit. The transaction will not be sent on to the issuer's bank and a response message is sent to the user to inform the user of the result. This response message should contain a suitable textual message to the user and instructions to the SIM application to handle cheque removal. In this case it is suitable to remove the cheque since it is not probable that the cheque will be possible to deposit at a later stage.

7. Issuer signature verification failure

   If the issuer's bank fails to verify the issuer's signature it is assumed that the user claiming to be the issuer is not or that the parameters has been corrupted during transit. The transaction will not be completed and an error message should be sent to the cheque's receiver's bank. A response message is sent from the receiver's bank to the user to notify the result. This response message should contain a suitable textual message to the user and instructions to the SIM application to handle cheque removal. In this case it is suitable to remove the cheque since it is not probable that the cheque will be possible to deposit at a later stage.

5.5 Withdraw cash

This section describes what happens when the user uses the service to make a cash withdrawal at an ATM. It covers the steps performed and the message sequence between the mobile phone / user, the pay-box, the ATM and the BFC gateway.

Unlike the payment scenario in the Retailer Mobile Payment Service only a "prepared" scenario is available in transactions with an ATM. The user can prepare the transaction in advance since the transaction is valid for a limited time (set to approximately 7-8 minutes in the pilot) after a correctly verified PIN-RSA.

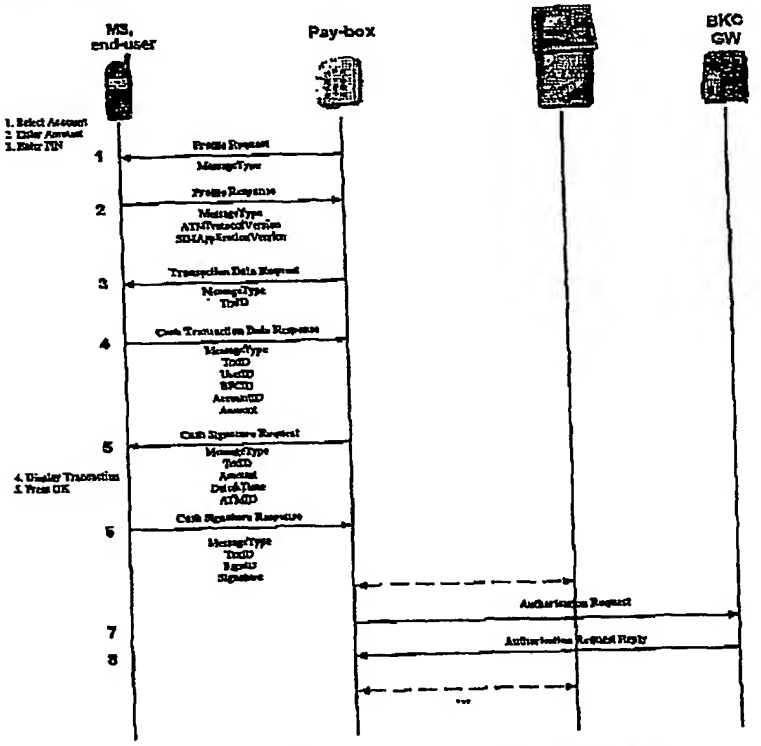

Figure 11: Message sequence during cash withdrawal.

5.5.1 Preparation

The user initiates the cash transaction by entering the ATM service menu and selects the appropriate menu entry. The user is requested to enter the amount of cash that should be withdrawn (see 6.1.2) and, if no default account is set, choose which account to withdraw from and is then asked to enter the PIN-RSA code. A correctly verified PIN is then valid for a limited period of time and will allow the transaction to be signed later on when the user continues the transaction at an ATM.

Note: The exact time period is dependent on the mobile terminal. From a security perspective it will be important to specify a maximum time limit, and from a usability perspective it will be important to specify a minimum time limit.

5.5.2 Message sequence

Before the message can be sent to the mobile phone the infrared connection must be established. To achieve this, the user activates the IR device on the terminal and points the infrared eye of the mobile phone towards the infrared eye of the pay-box.

1. Before the actual transaction is performed, the pay-box request information from the mobile phone on the characteristics of the application on the SIM card. This message is called Profile Request.

2. The SIM application responds with a Profile Response containing the profile information i.e. application and protocol version.

3. The pay-box sends a request to the mobile phone requesting transaction data. The message contains a transaction identifier, initiated in the pay-box, to be included in the message sequence to allow the pay-box to identify a session.

4. The SIM application responds with a message that includes the user's identifier, account information and the amount to be withdrawn. The transaction identifier received from the pay-box in previous message is also returned to pay-box.

5. The pay-box has knowledge of the ATM capabilities and processes the transaction data received from the mobile phone. This process involves confirming the requested amount and if necessary round off the requested amount to an amount supported by the ATM. The pay-box sends the confirmed amount, ATM identifier and date and time over the infrared connection to the mobile phone to be included in the signature with the rest of the information previously entered by the user.

   A summary of the cash transaction is then displayed on the mobile phone which the user is requested to confirm. The transaction information displayed includes the amount, the account nickname, date, ATM identifier and the reference number, which is the transaction identifier concatenated with the user's signature identifier. When the user has confirmed the transaction by pressing Yes/Ok, the application on the SIM card calculates a digital signature based on the private key and the transaction information according to the procedure in section 7.2.4.

6. The signed transaction is fetched from the mobile phone by the pay-box over the infrared connection. No further interactions will now take place with the mobile phone and the user can now await further instructions on the ATM display.

7. The pay-box sends the complete transaction including the digital signature to the BFC gateway.

8. The BFC gateway sends a response back to the pay-box after the transaction has been handled in the back-end systems. The response contains the result of the transaction and if successful the ATM dispenses the cash.

5.5.3 Error Cases, Withdraw cash

The following situations have been identified as error cases.

1. User not prepared

   If a user has not prepared the transaction before stepping up to an ATM, the SIM application will notify the user that no transaction is prepared and send an Error Indication message to the pay-box. The Error Indication will in this case indicate a temporary error to the pay-box.

2. Invalid amount

   The pay-box has some information regarding the capabilities of the ATM and uses this to acknowledge the amount parameter given by the user. If the user enters an amount that the ATM does not support, the pay-box adjusts the amount to the nearest smaller amount that is supported. This amount together with the other ATM information is sent this back to the user for confirmation in the signature request.

3. No cash in ATM

   If the amount parameter during a transaction is accepted by the pay-box but the ATM in reality does not support it e.g. a limited number of cash notes of a certain amount are remaining, the transaction will fail and the user will be informed via the display on the ATM.

4. No confirmation of transaction

   If the user leaves the ATM before confirming (pressing Ok/Yes) the transaction, the pay-box is left in a state where the next expected response is a signature. The next interaction, though, will probably be a new user wishing to perform a Profile Response. The new user will not be served until the timeout on the infrared communication link with the previous user has occurred (approximately 12 seconds after the previous user removed the mobile phone out of the range from the pay-box's IR device).

5. User cancels transaction

   Even though this is not a real error case it is mentioned here since it needs special attention. If the user cancels the transaction on the mobile phone either of two things can happen.

- The user remains within range of the pay-box's IR device and allows the cancel indication to be read by the pay-box. The pay-box can then perform the steps necessary to cancel the transaction and prepare for a new customer. If the same user stays, that user will be handled as a new customer and since a transaction probably not have been prepared the situation will generate a temporary error, as in User not prepared, in error case 1.
- The user leaves the ATM before the pay-box has managed to read the cancel indication. The pay-box and ATM are left in the same state as in error case 4 above, when a user leaves without confirming a transaction.

5.6 Withdraw cash from cheque / deposit cheque via ATM

This section describes what happens when the user uses the service to withdraw money from an ATM by using a mobile cheque. It covers the steps performed and message sequences between the mobile phone / user, the pay-box, the ATM and the BFC gateway.

Unlike the payment scenario in the Retailer Mobile Payment Service only a "prepared" scenario is available in transactions with an ATM. The user can prepare the transaction in advance since the transaction is valid for a limited time (set to approximately 7-8 minutes in the pilot) after a correctly verified PIN-RSA.

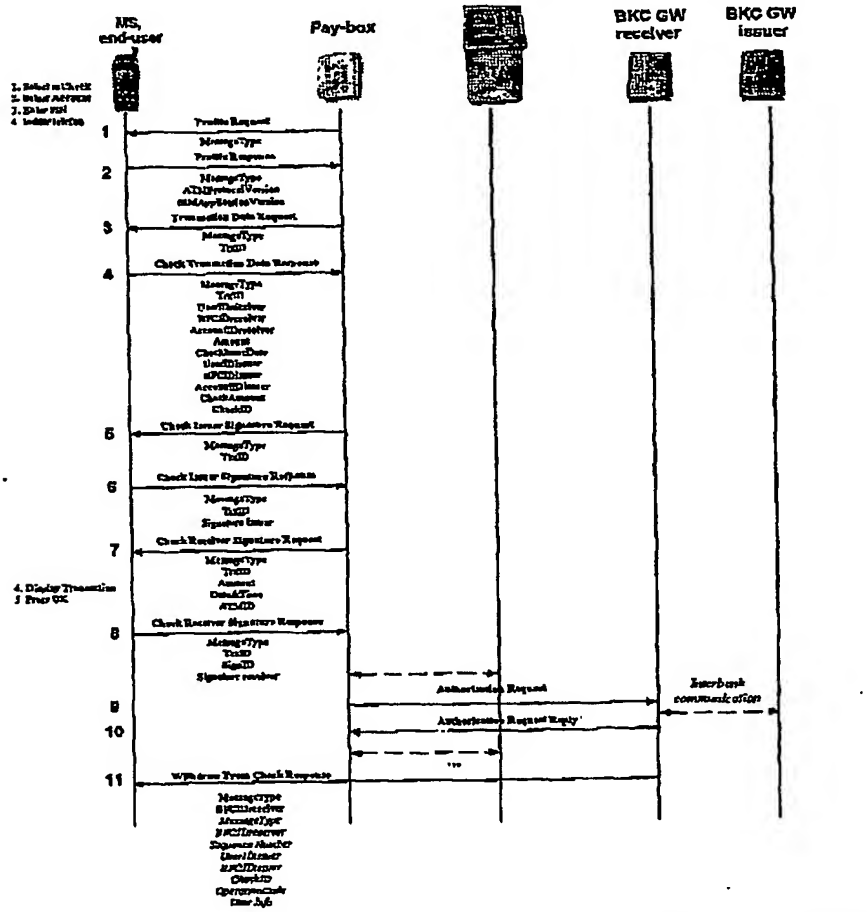

Figure 12: Message sequence during withdraw cash from cheque/deposit cheque via ATM.

5.6.1 Preparation

A received cheque can be withdrawn in cash from an ATM, fully, partially or no cash at all. The user can choose any amount less or equal to the amount issued on the received cheque.

The user enters the application via the appropriate menu entry in the application service menu and is presented with a list of all received cheques. In the next interactions the user chooses the cheque that should be used and the amount that should be withdrawn in cash (see 6.1.2).

If the amount of cash is equal to the cheque amount the user is prompted to enter the PIN-RSA code and when done the user is notified that the application is prepared to carry out the transaction at the ATM. A correctly verified PIN is valid for a limited period of time and will allow the transaction to be signed later on when the user continues the transaction at an ATM.

If the amount of cash differs from the cheque amount the user is prompted to choose an account, unless default account is set. When the account choice is made a summary with information on the amount to withdraw in cash and the amount to deposit to which account is displayed. When the summary is confirmed the user is prompted for the PIN-RSA and when done the user is notified that the application is prepared to carry out the transaction at the ATM.

Note: If the user wants to withdraw the whole amount, the user must choose an account anyway. This must be done to tie a user account to the transaction and to enable the bank to correct a failed transaction e.g. if the cash notes run out in an ATM the bank can correct the withdrawal on the user's account. It would seem confusing to the user to choose an account even if a cheque's whole amount was to be withdrawn and this is therefore solved automatically by using the default account, if one is set, or the first defined account in the account list if not.

A special case is if the user enters to withdraw no cash at all. In this case the whole cheque is deposited to the entered account. This means that an ATM also can be used to deposit a cheque to an account instead of doing it via SMS.

5.6.2 Message sequence

1. The message exchange starts with the pay-box requesting information from the mobile phone on the characteristics of the application on the SIM card.
2. The SIM application responds with the profile information i.e. application and protocol version.
3. The pay-box sends a request to the mobile phone requesting transaction data. The message contains a transaction identifier, initiated in the pay-box, to be included in the message sequence to allow the pay-box to identify a session.

4. The SIM application responds with a message that includes information about the receiver including, user identifier, account information and the amount to be withdrawn. Also included is information about the issuer of the cheque used, including user identifier, account identifier, cheque amount and cheque identifier.

5. The cheque issuer's signature is requested by the pay-box.

6. The cheque issuer's signature is fetched from the mobile phone by the pay-box over the infrared connection.

7. The pay-box has knowledge of the ATM capabilities and processes the transaction data received from the mobile phone. This process involves confirming the requested amount and if necessary round off the requested amount to a smaller amount supported by the ATM. The pay-box sends the confirmed amount, ATM identifier and date and time over the infrared connection to the mobile phone to be included in the signature with the rest of the information previously entered by the user.

   A summary of the cheque transaction is now displayed on the mobile phone and the user is requested to confirm. The transaction information displayed includes, the amount to withdraw, amount to deposit, nickname of account to deposit to, date when the cheque was issued and the information supplied by the pay-box. The pay-box transfers the date and time, ATM identifier and a transaction identifier that concatenated with the user's signature identifier is a reference number. When the user has confirmed the transaction by pressing Yes/OK, the application on the SIM card calculates a digital signature based on the private key and the transaction information according to the procedure in section 7.2.4.

8. The signed transaction is fetched from the mobile phone by the pay-box over the infrared connection. The transaction includes the cheque receiver's signature and signature identifier.

9. The pay-box sends the complete transaction including the digital signature to the BFC gateway.

10. The BFC gateway sends a response back to the pay-box after the transaction has been handled in the back-end systems. The response contains the result of the transaction and if successful the ATM dispenses the cash.

11. An application message is sent to the mobile phone from the receiver's bank to confirm that the withdraw cash from cheque request has been received. The message trigs the SIM application and displays a message informing the user of the result of the transaction. The application message also contains an operation code informing the application to either remove the cheque or keep the cheque. The bank defines both the message and operation code.

5.6.3 Error cases, Withdraw cash from cheque

The following situations have been identified as error cases.

1. User not prepared

   Same as error case 1 Withdraw Cash, section 5.5.3

2. Invalid amount

   Same as error case 2 Withdraw Cash, section 5.5.3

3. No cash in ATM

   Same as error case 3 Withdraw Cash, section 5.5.3

4. No confirmation of transaction

   Same as error case 4 Withdraw Cash, section 5.5.3

5. User cancels transaction

   Same as error case 5 Withdraw Cash, section 5.5.3

6. No cheque clearance on Issuer's account

   Same as error case 2 Deposit Cheque, section 5.4.3

7. Lost response message

   Same as error case 3 Deposit Cheque, section 5.4.3

8. Invalid cheque (already used)

   Same as error case 4 Deposit Cheque, section 5.4.3

9. Invalid cheque (validity time passed)

   Same as error case 5 Deposit Cheque, section 5.4.3

10. Receiver signature verification failure

    Same as error case 6 Deposit Cheque, section 5.4.3

11. Issuer signature verification failure

    Same as error case 7 Deposit Cheque, section 5.4.3

5.7 Management of the Mobile ATM Service

Management of the service involves both blocking operations, which require OTA mechanisms, and administration performed on the phone.

5.7.1 Blocking of Service

The user can choose to block the Mobile ATM Service if for example the phone has been lost or stolen and is in this case blocked in the phone

through an OTA blocking (also blocked in the BFC domain). The service is also blocked in the phone if an incorrect PIN-RSA is entered three times.

- Initiator: User
- Possible methods: Internet Bank, Phone call to customer care, Visiting customer care
- Actions: The service is blocked for usage in both the mobile phone and in the BFC domain.

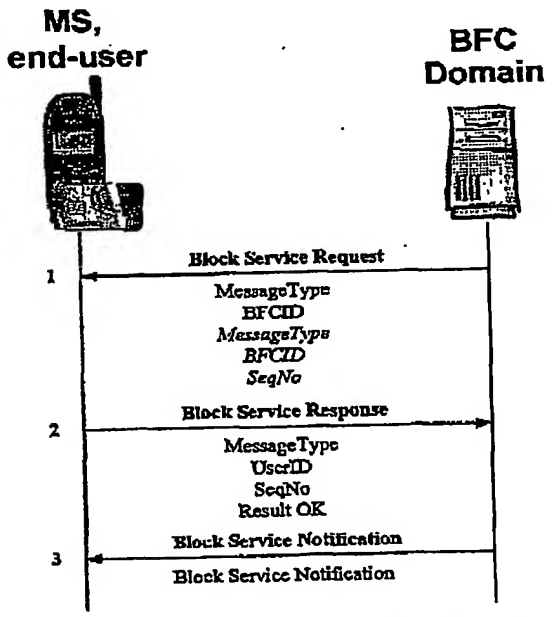

Figure 13: Message sequence flow during blocking of service

1. The BFC sends a request for blocking of the service. The message is signed as defined in section 7.2.3.
2. When the message is received, the SIM application verifies the signed message and validates the sequence number as defined in section 7.2.3. The BFCID is used to select which public key is used to verify the message.

   If the validation is successful, the service is blocked and the BFC domain is notified of the result. The sequence number received in the request from the BFC is returned in the response and could be used on the server side to link the result to the corresponding request.
3. Upon reception of the result, the BFC sends an ordinary short message to the mobile phone, to inform the user that the service has been blocked.

5.7.2 Blocking of Account

The bank can choose to block a certain account from use with the Mobile ATM Service, but the user can still use the service with other registered accounts.

- Initiator: Bank
- Possible methods: Bank Management System
- Actions: The account is blocked for usage in the BFC domain and in the mobile phone.

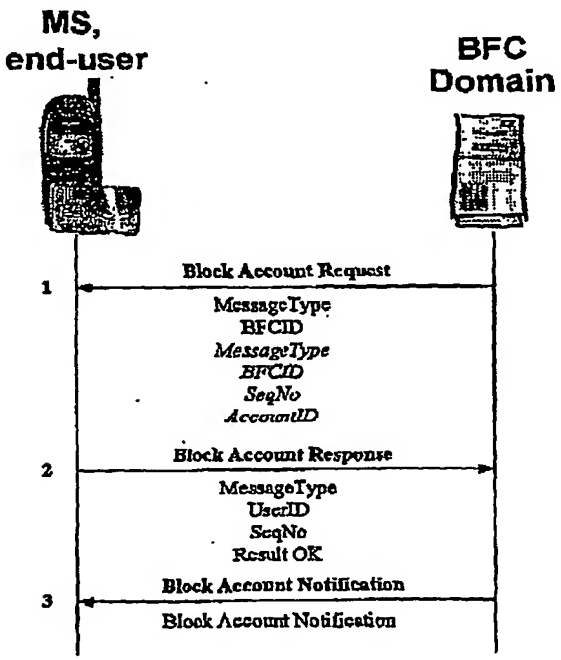

Figure 14: Message sequence flow during blocking of account

1. The BFC sends a request for blocking of an account. The message is signed as defined in section 7.2.3.

2. When the message is received, the SIM application verifies the signed message and validates the sequence number as defined in section 7.2.3. The BFCID is used to select which public key is used to verify the message.

   If the validation is successful, the account is blocked and the BFC domain is notified of the result. The sequence number received in the request from the BFC is returned in the response and could be used on the server side to link the result to the corresponding request.

3. Upon reception of the result, the BFC sends an ordinary short message to the mobile phone, used to inform the user that the account has been blocked.

5.7.3 Unblocking of Service

The user can unblock the Mobile ATM Service if it has been blocked.

- Initiator: User
- Possible methods: Internet Bank, Phone call to customer care, Visiting customer care
- Actions: If the service was blocked via an OTA blocking it is reactivated for usage in both the BFC domain and in the mobile phone. If the PIN-RSA was blocked the user is prompted by the application on the SIM card to select a new PIN.

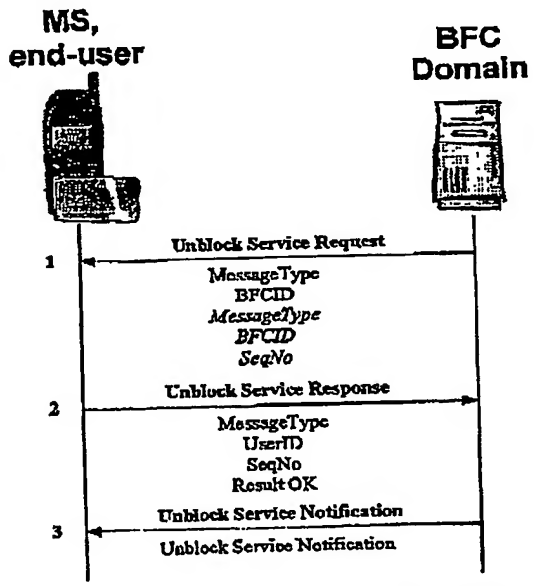

Figure 15: Message sequence flow during unblocking of service

1. The BFC sends a request for unblocking of the service. The message is signed as defined in section 7.2.3.
2. When the message is received, the SIM application verifies the signed message and validates the sequence number as defined in section 7.2.3. The BFCID is used to select which public key is used to verify the message.

   If the validation is successful, the service is unblocked in the phone and in the BFC domain (if it was blocked through an OTA update), or the user is prompted to select a new PIN-RSA (if the PIN was blocked)

and the service is then unblocked in the phone. The BFC domain is notified of the result. The sequence number received in the request from the BFC is returned in the response and could be used on the server side to link the result to the corresponding request.

3. Upon reception of the result, the BFC sends an ordinary short message to the mobile phone, used to inform the user that the service has been unblocked.

5.7.4 Unblocking of Account

The bank can make a previously blocked account available for use with the Mobile ATM Service.

- Initiator: Bank
- Possible methods: Bank Management System
- Actions: The account is reactivated for usage in the BFC domain and in the mobile phone.

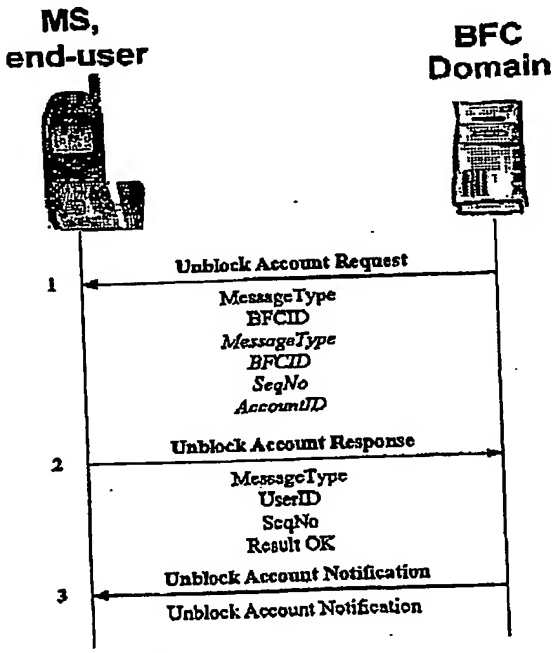

Figure 16: Message sequence flow during unblocking of account

1. The BFC sends a request for unblocking of an account. The message is signed as defined in section 7.2.3.
2. When the message is received, the SIM application verifies the signed message and validates the sequence number as defined in section

7.2.3. The BFCID is used to select which public key is used to verify the message.

If the validation is successful, the account is unblocked and the BFC domain is notified of the result. The sequence number received in the request from the BFC is returned in the response and could be used on the server side to link the result to the corresponding request.

3. Upon reception of the result, the BFC sends an ordinary short message to the mobile phone, used to inform the user that the account has been unblocked.

5.7.5 Changing PIN-RSA

The PIN-RSA can be changed in the phone through the Administration menu of the Mobile ATM Service. When changing the PIN, the user first has to enter the old PIN-RSA, and then enter the new PIN twice.

5.7.6 Setting Default Account

The user can choose to use a default account in the Mobile ATM Service if more than one account is registered. A default account is a "favorite" account that is likely to be used more often than other registered accounts and should therefore not have to be chosen every time.

If a default account is set the user will not have to choose account during a transaction and will see the nickname of the default account in subsequent transaction dialogs.

The default account setting is done during the registration phase using the Internet Bank, but the user can also change the default account later on through the Administration menu of the Mobile ATM Service in the mobile phone.

When setting the default account, the user is presented with a list of the registered account nicknames where the current default account is marked with a asterisk (*). A new default account can be set by scrolling to a new account nickname and press Yes/OK.

5.8 Transaction parameters

The following parameters are used in the transaction messages.

- AccountID

  This parameter contains an identifier that, within the domain of the BFC, uniquely identifies the account. In the pilot it will be possible to define a maximum of three accounts during the registration procedure.

- AccountNickname

  This parameter contains a string with the predefined bank indicator, for example SN for SparNord, followed by the nickname of the account defined by the end-user upon registration.

- Amount

  This parameter contains the amount to be withdrawn by the user from the bank account or from a cheque. The cheque consists of a value with a delimiter character ('.') between crowns and hundredth of a crown.

- ATMID

  This parameter contains a unique identifier for the ATM. The length of this identifier is eight digits.

- ATMProtocolVersion

  This parameter defines which version of the interface protocol is supported by the ATM Service application stored on the SIM card. The version number makes it possible for the pay-box to create different messages depending on the level of support in the SIM application.

- AuthenticationCode

  This parameter contains an authentication code which is used for client authentication purposes (in direction mobile phone to bank application) and for server authentication purposes (in direction bank application to mobile phone).

- BFCID

  This parameter contains a numeric value that is globally unique and indicates which BFC is responsible for handling the payment transaction.

- BFCPublicKey

  This parameter contains the public key of the BFC.

- ChequeAmount

  This parameter contains the value of a cheque. The parameter consists of two parts, the value and the currency indicator.

- ChequeID

  This parameter contains a numeric value assigned by the application on the SIM card, which uniquely identifies a particular cheque from the end-user perspective.

- ChequeIssueDate

  This parameter contains the date when the cheque was issued as an 8-digit long date stamp in the format YYYYMMDD. The value of this parameter is provided by the SMS GW/proxy.

- Date&Time

This parameter contains a 14 digit long timestamp for the transaction in the format YYYYMMDDHHMMSS.

- DefaultAccountInfo

  The DefaultAccountInfo indicates which account the user has defined as default account during the registration procedure.

- End-UserPublicKey

  This parameter contains the public key of the end-user.

- ErrorCode

  This parameter contains an error code informing the SIM application that an error has occurred.

- MessageReference

  This parameter contains a reference number that together with the identity of the user is used to link different messages belonging to the same concatenated application message to each other.

- MessageType

  This parameter contains a numeric value that identifies which type of message it is.

- MSISDNIssuer

  This parameter contains the mobile phone number of the issuer of the cheque, in International format represented as a string of decimal digits without the International prefix ("+","00").

- MSISDNreceiver

  This parameter contains the mobile phone number of the receiver of the cheque, in International format represented as a string of decimal digits without the international prefix ("+", "00").

- OperationCode

  This parameter indicates which action the SIM application shall perform upon reception of the response on a deposit or a withdrawal request. The value of this parameter is set by the bank and depends on the outcome of the processing of the transaction at the bank.

- OTAProtocolVersion

  This parameter defines which version of the OTA interface protocol that is supported by the MPS SIM application.

- ResultCode

  This parameter defines the result of the execution of the request.

- SeqNo

  The Sequence Number is a numeric value generated by the BFC, which must be incremented for each new OTA operation that the BFC requests towards a specific user, i.e. a separate counter is used for each user. Must not be equal to zero (0).

- Signature

  This parameter contains the digital signature calculated by the application on the SIM card.

- SignID

  This parameter contains a numeric value assigned by the application on the SIM card, which uniquely identifies the transaction from the user perspective. The SignID is incremented by one for each transaction that is signed by the user and it is used in the BFC domain to prevent replay attacks.

- SIMApplicationVersion

  This parameter contains the version number of the ATM Service application stored on the SIM card. It is passed on to the BFC domain to allow for future changes in the service.

- TrxID

  This parameter contains a numeric value assigned by the pay-box, which uniquely identifies the transaction from the pay-box perspective. This parameter is then passed on in every request and response in the session, which makes it possible for the pay-box to manage multiple transactions.

- UserID

  The UserID uniquely identifies the user within the BFC domain. This could be an arbitrary identifier assigned by the BFC or for example the mobile phone number (MSISDN).

- UserInfo

  This parameter contains a textual message intended for the end-user and is defined by the bank.

6 User Interactions

In this chapter different interactions from the previous user scenario chapter that need extra attention, are discussed.

6.1 Input of amount

In the SDC Mobile ATM Service there are several user scenarios that require the user to enter an amount. These include the situations when the user issues a cheque to be sent via SMS and when a cheque or cash transaction is performed at an ATM.

The case when the transaction is performed at an ATM is special in the sense that the pay-box is informed about the capabilities of the ATM and can therefore round off an amount entered by the user. If for example the user enters the amount 563, the pay-box "knows" that the ATM at this time only can supply bills of the amount 100 and asks the user to confirm a withdrawal of 500.00 DKK.

6.1.1 Issue cheque

A mobile cheque supports any amount bigger than 0.00 (DKK in pilot) and this requires the user to be able to enter an amount delimited by a decimal point. The decimal point is entered as either an asterisk (*) or square ('#') which delimits between crowns and hundredths of a crown e.g. 249*50. The total length of the input can be at most eleven characters, ten digits plus the character '*' (or '#').

The cheque's amount can also be entered in whole crowns and in this case the length of the input can be at most eight digits.

The figure below summarises accepted and unaccepted input during an Issue Cheque transaction with some examples.

Entered Amount	***Result***	***Comment***
*	NOK	Error indication from SIM application.
**	NOK	Error indication from SIM application.
0	NOK	Error indication from SIM application.
*5	OK	Amount shown in subsequent dialogs: 0.50 DKK
*50	OK	Amount shown in subsequent dialogs: 0.50 DKK
0*50	OK	Amount shown in subsequent dialogs: 0.50 DKK
0*500	NOK	Error indication from SIM application.

145	OK	Amount shown in subsequent dialogs: 145.00 DKK
0145	OK	Amount shown in subsequent dialogs: 145.00 DKK
145*	OK	Amount shown in subsequent dialogs: 145.00 DKK
145*0	OK	Amount shown in subsequent dialogs: 145.00 DKK
145*03	OK	Amount shown in subsequent dialogs: 145.03 DKK
145*030	NOK	Error indication from SIM application
12345678	OK	Amount shown in subsequent dialogs: 12345678.00 DKK
123456789	NOK	Error indication from SIM application
12345678*500	NOK	Error indication from ME, Input length too long

Figure 17: Input during Issue Cheque transaction

All input unaccepted by the SIM application is reported as erroneous by the application.

6.1.2 Cash or cheque transaction at an ATM

The input is handled in the exact same way as in the *Issue Cheque* case above with two important differences.

- The amount shown in the subsequent dialogs on the mobile phone, after the user has entered the requested amount, will depend on what the pay-box has been informed that the ATM support.
- If the entered amount is 0 and it is a "*Withdraw cash from cheque*" transaction the input is accepted and treated as a special case of depositing a cheque. The transaction will in this case be a deposit of the cheque's whole amount to the account.

The figure below summarises accepted and unaccepted input during an ATM transaction with some examples.

Entered Amount	***Result***	***Comment***
*	NOK	Error indication from SIM application

0	NOK/OK	In case it is a "*Withdraw cash from account*" transaction the amount is unaccepted by the SIM application. In case it is a "*Withdraw cash from cheque*" transaction it is treated as a special case of depositing a cheque. Amount shown in subsequent dialogs: 0.00 DKK i.e. no cash withdrawal and the whole amount of the cheque will be deposited to the account.
*5	OK	Amount shown in subsequent dialogs is dependent on pay-box.
*50	OK	Amount shown in subsequent dialogs is dependent on pay-box.
0*50	OK	Amount shown in subsequent dialogs is dependent on pay-box.
0*500	NOK	Error indication from SIM application
145	OK	Amount shown in subsequent dialogs is dependent on pay-box.
145*	OK	Amount shown in subsequent dialogs is dependent on pay-box.
145*0	OK	Amount shown in subsequent dialogs is dependent on pay-box.
12345678	OK	Amount shown in subsequent dialogs is dependent on pay-box.
123456789	NOK	Error indication from SIM application
12345678*500	NOK	Error indication from ME, Input length too long

Figure 18: Input during ATM transactions

Note: The table lists input accepted and unaccepted from the SIM application's (and ME) point of view. An entered amount can be accepted by the application but be rejected by the pay-box depending on what the ATM supports at that specific time. In these situations the pay-box adjusts the user-requested amount to an amount that is supported by the ATM.

6.2 Input of telephone number

In the SDC Mobile ATM Service there is one scenario that require the user to enter a telephone number. In this scenario the issuer enters the telephone number (MSISDN) of the receiver to allow the cheque to be sent via SMS.

The telephone number to the receiver must be entered in international format i.e. leading '+' sign and country code followed by the national number. The SIM application will pre-enter the string "+45" to the input field to simplify this procedure.

The input must be between 8 and 16 digits (including "+45") and must not contain any special characters like, '*', '#' or more than one '+', starting the string.

The figure below summarises accepted and unaccepted number input during an Issue Cheque transaction with some examples.

Entered Phone Number	***Result***	***Comment***
+45*1234	NOK	Error indication from SIM application:
*4512345	NOK	Error indication from SIM application:
45123456	NOK	Error indication from SIM application:
+451234	NOK	Error indication from ME, Input length too short
+4512345678901234	NOK	Error indication from ME, Input length too long
+4612345	OK	
+45123456789012	OK	
+299123456789012	OK	
+451234567890123	OK	Note: This number is accepted by the SIM application. However, the representation of UserID currently used restricts the national part of the number to a maximum of 12 digits. This gives that a cheque issued for this number will not be possible to deliver, since the receiver can not be a user of the service.

Figure 19: Telephone number input during Issue Cheque transaction

6.3 Handling of mobile cheques

6.3.1 Issued cheques

A mobile cheque can be issued as soon as the user has completed the ATM service activation procedure. If the service is blocked, PIN is blocked or all accounts are blocked, a cheque can not be issued and it is up to the user to perform the steps necessary to put the service in an active state again.

When a cheque is issued and sent to the receiver it is stored in a separate file with other sent cheques and it is presented in the issuer's application's *Issued* cheque list. This list is a cyclic list of fixed size, initially set to five cheques. If the file is full, the oldest sent cheque is overwritten when the next cheque is issued.

The list is intended to be used to review previously sent cheques and to send a cheque again in case it is lost on its way to the receiver, which for example could be caused by the operator's SMS-C malfunctioning or a connection to it being down. Two operations are possible on previously sent cheques in the list, *Show* and *Send again*.

Note: The information stored for each issued cheque is the information that has been signed and not the signature itself. This approach minimises the storage overhead but yet allows the same identical cheque to be re-sent with a re-calculated signature.

6.3.2 Received cheques

A mobile cheque can be received as soon as the user has completed the ATM service activation procedure. If the service is blocked, PIN is blocked or all accounts are blocked, a cheque is still received and stored in the received cheque SIM file. It can however not be viewed, deposited or withdrawn, since the service is unavailable, and it is up to the user to perform the steps necessary to make the service work again and then the received cheques will be possible to use.

When the user receives a mobile cheque, a notification is displayed on the mobile phone and the cheque is stored in a file on the SIM card with other received cheques. This file is a non-cyclic fixed size file, initially set to five cheques. A new cheque can not be received if the file is full and therefore when a cheque is saved to the last empty position a message is displayed to the user informing that action should be taken. The only ways to make room for further incoming cheques are to deposit or withdraw one or more of the received cheques.

If a cheque already is stored at the receiver and an identical cheque is received again i.e. the issuer of the cheque uses the *Resend* command on the previously issued cheque, only the last received cheque will be stored by the SIM application. In this way the SIM application clears the cheque storage from unnecessary cheques since only one of the cheques will be able to deposit or withdraw anyway. The SIM application uses the cheque identifier together with the user identifier to find identical cheques.

The file containing received cheques is presented to the user by entering the application with the appropriate menu entry. The *Received* cheque list is used to view and deposit received cheques with the operations, *Show* and *Deposit*.

Note: A cheque is removed from the SIM file when the application message (Cheque Deposit Response or Withdraw From Cheque Response) is received from the receiver's bank domain after a transaction has been completed. The user is not notified of the cheque removal.

7 Security Overview

7.1 General Security Concepts

7.1.1 Asymmetric Encryption

Asymmetric encryption systems, or public key systems, use two different keys, a public and a private key, for encryption and decryption. The two keys are dependent on each other and form a personally unique key pair, but it is not possible to calculate one key from knowledge of the other.

Either the public or the private key can be used for encryption. The decryption is then made with the corresponding key of the key pair. For example, a message encrypted with a recipient's public key can be decrypted only with the same recipient's private key.

The RSA algorithm is today a de facto standard for public key systems.

7.1.2 Hash Algorithms

Hash algorithms are used to create a digital fingerprint, or a message digest of a certain piece of information. Even the slightest change in the original message document produces a completely different digital fingerprint.

A MAC (Message Authentication Code) is a hashed message encrypted using a symmetric key. A MAC gives message integrity but not non-repudiation.

SHA-1 is a commonly used hash algorithm. It produces a 20-byte message digest of any input message.

7.1.3 Digital Signatures

A digital signature is created in the following way:

1. The message is hashed with a hash algorithm (i.e. SHA-1) and the digital fingerprint of the text is created.
2. The fingerprint is encrypted with the sender's private key.
3. The result is a signature that is unique for every combination of message and private key.

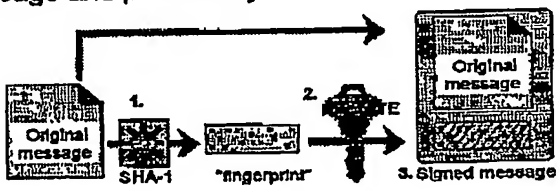

Figure 20: Digital signature calculation

Upon reception the digital signature is verified in the following way:

1. The original message is run through the same hash algorithm as used when signing.
2. The signature is decrypted with the sender's public key.
3. The two results are compared. If they are identical, the digital signature is valid.

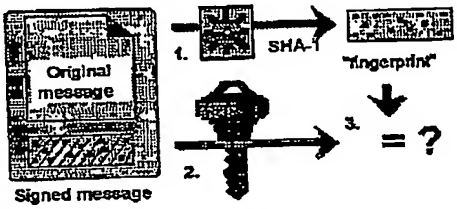

Figure 21: Digital signature verification

Digital signatures provide the following:

- Authentication of the sender's identity.
- Assurance that any changes to the message will be noticed (integrity).
- Assurance that the sender can not deny sending the message (non-repudiation).

7.2 Mobile ATM Service security

In the Mobile ATM Service the concepts introduced above are used to create secure transactions.

7.2.1 RSA Keys

During the activation process of the service, an RSA key pair is generated on the SIM card. The private key is stored in a tamperproof area on the SIM card, and the public key is exported from the mobile phone to the server in the BFC domain. In return, the server sends its own public RSA key to the mobile phone.

All RSA keys (both end-user and BFC keys) have a 1024-bit modulus and a public exponent set to 2^16+1 (=65537).

7.2.2 Public Key Exchange

During the activation process of the service, a 1024-bit RSA key pair is generated on the SIM card. The private key is stored in a tamperproof area on the SIM card, and the public key is exported from the mobile phone to the server in the BFC domain.

In order for the server to be able to authenticate the sender of the public key, the user has previously received a One-Time-Password (OTP) from the server on a secure, separate channel (Internet Bank). The application on the SIM card calculates a message digest using SHA-1. The input is a concatenated string of all the information sent in the message (including the public key) and the OTP. The generated message digest is 20 bytes,

but it is truncated to the first 8 bytes to create an Authentication Code. See figure below.

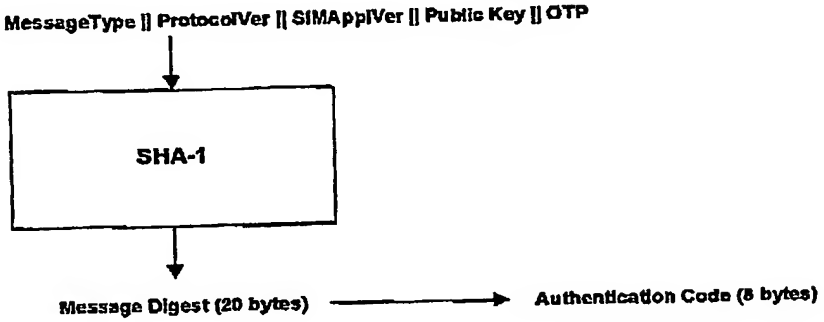

Figure 22: Authentication Code calculation on user's public key

The public key together with the other information and the Authentication Code are exported to the BFC domain. The total length of the message will be 139 bytes (1 byte Message Type + 1 byte Protocol Version + 1 byte SIM Application Version + 128 bytes Public Key + 8 bytes Authentication Code), which can be sent in one SM.

The server can then calculate an Authentication Code in the same way on the known OTP and the received information. If the comparison with the received Authentication Code is successful, it can be assumed that the public key has not been corrupted during transfer and that it indeed originates from the user.

If the public key of the user is accepted the server sends the public key belonging to the BFC domain, which will be used for server authentication purposes in subsequent operations. The message contains a new Authentication Code, which makes it possible for the application on the SIM card to verify that the message is originated from the correct source. It also contains the BFCID, which is used by the phone to link the public key to the correct BFC (in a multiple BFC scenario).

The Authentication Code is again the first 8 bytes of a message digest calculated using SHA-1. The input is a concatenated string of all the information sent in the message (including the public key) and the OTP. See figure below.

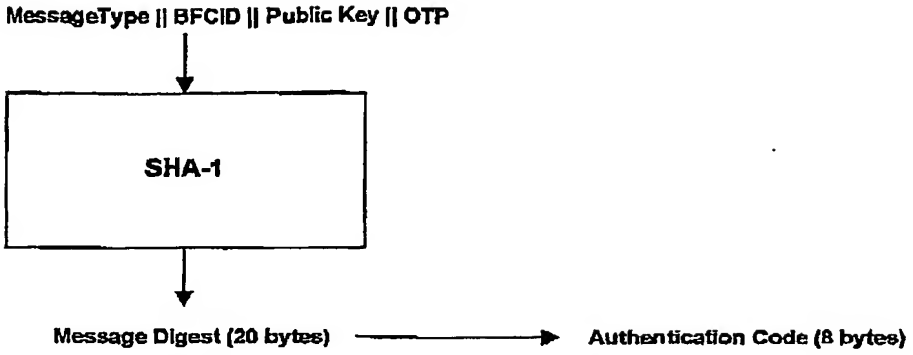

Figure 23: Authentication Code calculation on BFC's public key

The public key together with the other information and the Authentication Code are sent to the mobile phone. The total length of the message will be 138 bytes (1 byte Message Type + 1 byte BFCID + 128 bytes Public Key + 8 bytes Authentication Code), which can be sent in one SM.

The application on the SIM card can then calculate an Authentication Code in the same way on the known OTP and the received information. If the comparison with the received Authentication Code is successful, it can be assumed that the public key has not been corrupted during transfer and that it indeed originates from the BFC.

7.2.3 Server Authentication

In order for the mobile phone to be able to trust OTA updates and requests from the BFC domain, a mechanism for server authentication is needed.

All information in messages from the server is encrypted using RSA with the BFC's private key according to PKCS#1 (Public Key Cryptography Standards) described in Ref. [1]. This creates a signature, which makes it possible for the application on the SIM card to perform server authentication upon reception of the message.

In addition to the application information, the signed message contains the Message Type, the BFC identifier and a sequence number.

Note: The Message Type and the BFC identifier are also sent unencrypted to the mobile phone, as they are needed by the SIM application before the signed message has been verified (decrypted). The Message Type is used to determine how the message should be handled. The BFC identifier is used to select which public key should be used to decrypt the message.

The sequence number is a 3-byte integer generated by the BFC, which must be incremented for each new operation that the BFC requests towards a specific user, i.e. a separate counter is used for each user.

Before the encryption operation, the information has to be padded to 128 bytes.

The padding is done using an adaptation of the EMSA-PKCS1-v1_5 encoding operation described in Ref. [1]. Since no hash of the message is calculated, the hash algorithm identifier will not be included.

Basically, the padding is performed in the following way:

1. Construct a padding string consisting of (128-[length in bytes of data to sign]-3) octets with the hexadecimal value FF.
2. Concatenate the padding string, the message to be signed, and delimiters to form the padded message:

   00 || 01 || FF FF [...] FF FF || 00 || [message]

The padded message is then signed by the BFC by encrypting the information with the private key of the BFC. See figure below.

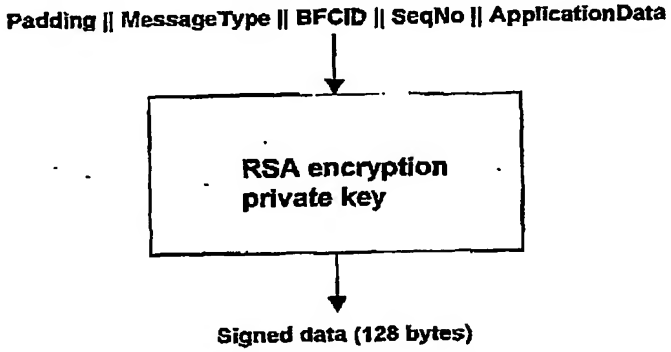

Figure 24: Server authentication with private RSA transformation

When the message is received, the SIM application performs the following steps:

1. The message is decrypted using RSA with the BFC's public key. The BFCID is used to select which public key is used to decrypt the message.
2. The padding is chequeed to verify that the information has not been changed after it was signed, and then removed to recover the signed data. (For additional security, the BFCID and the Message Type in the signed message can also be compared to the BFCID and the Message Type that were sent unencrypted to verify that the information has not been changed.)
3. The sequence number is compared to the sequence number received with the latest OTA request, in order to prevent replay attempts. The number must be incremented by the server for each new OTA request.

7.2.4 Transaction Signing

Mobile transactions initiated by the user are signed and can be listed as follows:

- Issue cheque (via SMS)
- Deposit cheque (via SMS)
- Withdraw cash (via ATM)
- Withdraw/deposit from cheque (via ATM)

The transactions are signed using RSA according to PKCS#1 (Public Key Cryptography Standards) described in Ref. [1].

7.2.4.1 Transaction parameters

This section outlines the parameters and their order as they are signed during the transaction. The SHA-1 hash is calculated on the following concatenated data in each transaction.

The size and format of each parameter is defined in Ref. [**Fejl! Henvisningskilde ikke fundet.**]. When input to the signature calculation, the parameters are all given in full length with any unused bytes set according to Ref. [**Fejl! Henvisningskilde ikke fundet.**]. However, the AccountID is represented as 1 full byte with leading bits set to zero in the signature calculation.

7.2.4.1.1 Issue cheque

MSISDN_receiver	(20 bytes)
BFCID_issuer	(1 byte)
AccountID_issuer	(1 byte)
ChequeAmount	(15 bytes)
ChequeID	(3 bytes)

The format on MSISDNreceiver when signed is the complete international phone number, entered by the user, without the leading '+' or "00" string.

7.2.4.1.2 Deposit cheque

BFCID_receiver	(1 byte)
AccountID_receiver	(1 byte)
SignID	(3 bytes)
ChequeIssueDate	(8 bytes)
Signature_Issuer	(128 bytes)

In the transaction summary a 7-digit reference number (RefNo) is displayed to the user. The RefNo is usually a 4-digit transaction identifier (TrxID) concatenated with the user's 3-digit signature identifier (SignID). During a deposit cheque transaction, however, no interaction with a pay-box takes place and no TrxID can therefore be received. To keep the RefNo in a uniform format to the user the TrxID is in this operation replaced with a dummy value ("0000") which is not signed.

7.2.4.1.3 Withdraw cash

BFCID	(1 byte)
AccountID	(1 byte)
Amount	(15 bytes)
SignID	(3 bytes)
TrxID	(4 bytes)
Date&Time	(14 bytes)
ATMID	(8 bytes)

The user signs the TrxID, received from the pay-box, and the SignID. These parameters are displayed to the user in the transaction summary as a 7-digit reference number, RefNo, which is TrxID concatenated with SignID (TrxID || SignID).

7.2.4.1.4 Withdraw/deposit from cheque

BFCID_receiver	(1 byte)
AccountIDreceiver	(1 byte)
AmountToWithdraw	(15 bytes)
SignID_receiver	(3 bytes)
ChequeIssueDate	(8 bytes)
TrxID	(4 bytes)
Date&Time	(14 bytes)
ATMID	(8 bytes)
Signature_Issuer	(128 bytes)

The user signs the TrxID, received from the pay-box, and the SignID. These parameters are displayed to the user in the transaction summary as a 7-digit reference number, RefNo, which is TrxID concatenated with SignID (TrxID || SignID).

7.2.4.2 Signature calculation

The 20-byte result of the SHA-1 operation above is then padded to 128 bytes and encrypted using RSA with the user's private key.

The padding is done according to the EMSA-PKCS1-v1_5 encoding operation described in Ref. [1].

Basically, the padding is performed in the following way:

1. Hash the message using SHA-1.
2. Construct a SHA-1 hash algorithm identifier using DER (Distinguished Encoding Rules). This results in the following octet string:

   30 21 30 09 06 05 2b 0e 03 02 1a 05 00 04 14
3. Construct a padding string consisting of 90 octets with the hexadecimal value FF.
4. Concatenate the padding string, the algorithm identifier, the hashed message, and delimiters to form the padded message:

   00 || 01 || FF FF [...86xFF...] FF FF || 00 || 30 21 30 09 06 05 2b 0e 03 02 1a 05 00 04 14 || [hashed message]

The signature verification is done in the following way:

1. Hash the original transaction using SHA-1 and apply the padding described above.
2. Decrypt the signature using RSA and the user's public key.
3. Compare the hashed and padded transaction with the decrypted signature. If they match, the signature is valid.

Generally, it should be noted that point-to-point communication between a mobile station (mobile telephone) and another mobile station and/or a cash-dispensing machine (automatic teller machine) can be in accordance with the IrDA or fast IrDa standard, the Bluetooth standard and/or any other near-range communication standard.

Generally, the mentioned pay-box can be an integrated part of a cash-dispensing machine (automatic teller machine, ATM).

CLAIMS

1. A method of issuing an electronic payment cheque, the method comprising the steps of:

in a mobile station, prompting a user to confirm issue of a payment cheque, and transmitting cheque information, with a digital signature, to a receiver being identified by a subscriber number.

2. A method according to claim 1, wherein the cheque information is transmitted via a message proxy.

3. A method according to claim 2, wherein the cheque information is converted at the message proxy to an SMS Point-to-point download message, which is transmitted to the receiver.

4. A method of making an electronic cheque deposit, the method comprising the steps of:

in a mobile station, receiving cheque information with a signature of a cheque issuing user, wherein the receiver is identified by a subscriber number,

prompting a cheque receiving user to confirm the cheque information by applying a personal signature,

transmit the cheque information with the signature of the cheque issuing user to an identified bank gateway of the cheque receiving user;

transmit the confirmed cheque information to the identified bank gateway cheque issuing user for payment transfer.

5. A method according to claim 4 wherein the cheque information is received at the mobile station by means of infrared or radio point-to-point communications.

6. A method according to claim 4 wherein the cheque information is received at the mobile station by means of a service provided by a network operator.

7. A method according to claim 4 wherein the service is a Short Message Service.

8. A method of processing a request for withdrawal of cash, the method comprising the steps of:

In a mobile station, a request for cash withdrawal with a user identifier and an amount is transmitted to an automatic teller machine;

In the automatic teller machine, the request can be verified in respect of the amount, subsequently, a request for confirmation is sent from the automatic teller machine to the mobile station, where the user can confirm the requested cash withdrawal and/or a cash withdrawal suggested by the automatic teller machine; the withdrawal is confirmed by applying a digital signature of the user;

the automatic teller machine transmits information of the cash withdrawal to a bank gateway of the user's bank;

the automatic teller machine waits for response from the bank gateway to dispense cash to the user.

9. A method according to claim 8, further comprising the steps of:

from the automatic teller machine, transmitting a request for a profile of the mobile station, and in response thereto providing a profile to the automatic teller machine;

transmitting a request with transaction ID to mobile phone for transaction data.

10. A method according to claim 8 wherein the information between the mobile station and the automatic teller machine is communicated by means of infrared or radio point-to-point communications.

11. A method of processing a request for withdrawal of cash from an electronic cheque, the method comprising the steps of:

in a mobile station, a request for cash withdrawal with a user identifier of a user that has received an electronic cheque, an amount, an identifier of the user that has issued the cheque and an identifier of the cheque is transmitted to an automatic teller machine(4);

subsequently, a digital signature of the issuer of the cheque is requested by the automatic teller machine and is fetched from the mobile station (5,6);

the automatic teller machine verifies the request in respect of the amount, subsequently, a request for confirmation is sent from the automatic teller machine to the mobile station, where the user can confirm the requested cash withdrawal and/or a cash withdrawal suggested by the automatic teller machine; the withdrawal is confirmed by applying a digital signature of the user (7);

the signed transaction is fetched from the mobile station by the automatic teller machine (8);

the automatic teller machine transmits information of the cash withdrawal to a bank gateway of the bank of the receiver of the cheque (9);

the automatic teller machine waits for response from the bank gateway to dispense cash to the receiver of the cheque (10).

12. A method according to claim 11 further comprising the step of: transmitting a response from the bank gateway of the receivers bank to confirm that the withdraw cash from the cheque request has been received (11).